IN THE SPECIFICATION

Please rewrite the following paragraph on page 1, lines 4-12:

The present application relates to:

U.S. Patent Application Serial No. 09/793,239, now U.S. Pat. No. 6,823,464, entitled "Method of Providing Enhanced Security in a Remotely Managed Computer System"; 9/19/05

U.S. Patent Application Serial No. 09/931,550, still pending ~~[Attorney Docket No. RPS9-2001-0042]~~, entitled "System Management Interrupt Generation Upon Completion of Cryptographic Operation"; and 9/19/05

U.S. Patent Application Serial No. ~~09/_____ [Attorney Docket No. RPS9-2001-0046~~ 09/931,629, still pending, entitled "Flash Update Using A Trusted Platform Module," which are hereby incorporated by reference herein. 9/19/05

medium upon which it is stored so that the medium carries computer readable information. The change may be electrical, magnetic, chemical, biological, or some other physical change. While it is convenient to describe the invention in terms of instructions, symbols, characters, or the like, the reader should remember that all of these and similar terms should be associated with the appropriate physical elements.

Note that the invention may describe terms such as comparing, validating, selecting, identifying, or other terms that could be associated with a human operator. However, for at least a number of the operations described herein which form part of at least one of the embodiments, no action by a human operator is desirable. The operations described are, in large part, machine operations processing electrical signals to generate other electrical signals.

The present invention is described with respect to the update of a BIOS image within a data processing system, such as system 313. However, the present invention is applicable to the update of any data and/or image within an information handling system.

The present invention makes use of the TCPA (Trusted Computing Platform Alliance) Specification where a trusted platform module (TPM) 351 has been installed within system 313. The TCPA Specification is published at ~~www~~.trustedpc.org/home/home.htm, which is hereby incorporated by reference herein. However, it should be noted that the present invention may also be implemented using other cryptographic verification methods and processes.

System 313, either automatically, or as a result of input from a user, will begin a process where the BIOS image is to be updated. Such a BIOS image may reside within ROM 316 or some other memory module within system 313. The update of the BIOS image may be received over a network 350 or on a diskette.

Referring to FIGURE 2, the process begins when a flash utility requests flash unlock from the system software (e.g., BIOS). After the system software has verified the authenticity and authorization of the flash utility, in step 201, it will post a message to BIOS using a secure messaging protocol and unlock the flash memory (excluding the

boot block code). Posting of the message may be performed using a process as described in cross-referenced Patent Application Serial No. 09/793,239, now U.S. Pat. No. 6,823,464 In step 202, the flash update utility will update the BIOS image in the flash memory and relock the flash (either directly or via a call to the BIOS).

Referring to FIGURE 1, on a subsequent re-boot (either warm or cold), the BIOS boot block code in POST will inspect the message buffer noted above to determine if the message indicates that the BIOS flash images has been previously updated. If in step 102, the update message is present, then in step 104, the boot block code will then perform a signature verification on the next block of code to be executed. In step 105, if the signature verifies correctly, then the boot block code will store the new hash in non-volatile, secure storage (step 108), extend the appropriate PCR (register) with the new hash, and pass control to the next code block in POST in step 107. If the signature does not verify, then in step 106, the boot block code will suspend the boot process and indicate the failure via some alert mechanism.

In step 102, if an update message is not present, then in step 103, POST will retrieve and extend the appropriate TPM PCR using the hash that was stored at step 108. Next, the process will continue with POST in step 107.

As is apparent from the description of this process, the flash EEPROM and the system utilities that provide access to the flash EEPROM must be protected from tamper. Numerous methods may be used to accomplish the needed protection. For instance, hardware circuits that provide notification to a secure system function may be incorporated in the system design to prevent unauthorized access to the flash EEPROM. One such implementation is described in U.S. Patent Application Serial No. 09/953,775, now U.S. Pat. No. 6,711,690 ~~[Attorney Docket No. RPS9-2001-0113]~~, which is incorporated by reference. Additional hardware may be required to provide protection to the system function that performs the signature verification of the new BIOS image and related utilities.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made